EXCEPTIONAL P-GROUPS OF ORDER P^5

SICHAO JIANG

ABSTRACT. The mininal degree of a finite group G, $\mu(G)$, is defined to be the smallest natural number n such that G embeds inside $\mathrm{Sym}(n)$. The group G is said to be exceptional if there exists a normal subgroup N such that $\mu(G/N) > \mu(G)$. We will investigate the smallest exceptional p-groups, when p is an odd prime. In [5] Lemiuex showed that there are no exceptional p-groups of order strictly less than p^5 and imposed severe restrictions on the existence of exceptional groups of order p^5. In fact he showed that if any were to exist, they must come from central extensions of four isomorphism classes of groups of order p^4. Then in [3] he exhibited an example of an exceptional group of order p^5. The author demonstrates the existence of two more exceptional groups arising in such a fashion and rules out the possibility of the remaining case.

1. INTRODUCTION

For the purposes of this paper, all groups will be assumed to be finite. The *minimal degree* $\mu(G)$ of a group G, is the least non-negative integer n such that G embeds inside $Sym(n)$. That is, it is the smallest possible faithful permutation representation of G. Define two permutation representations of G by $\phi : G \longrightarrow Sym(X)$ and $\psi : G \longrightarrow Sym(Y)$. We say that ϕ and ψ are *equivalent* if there exists a bijection $\theta : X \longrightarrow Y$ such that the following diagram communtes:

$$
\begin{array}{ccc}
X & \xrightarrow{g\phi} & X \\
\downarrow{\theta} & & \downarrow{\theta} \\
Y & \xrightarrow{g\psi} & Y
\end{array}
$$

which is equivalent to saying that

$$[x(g\phi)]\theta = (x\theta)g\psi, \quad \text{for all } x \in X.$$

Now let H be a subgroup of G. The *core* of H in G, denoted $\mathrm{core}H$, is the largest normal subgroup of G contained in H. In particular if $H \lhd G$, then $\mathrm{core}H = H$.

Now we will make the most important construction of this section. We will define a permutation representation of G by the group $Sym(G/H)$ for some subgroup $H \leq G$ and show that in fact every transitive permutation

representation of G is equivalent to such a representation. Let H be a subgroup of G. Let $G/H = \{Hx \mid x \in G\}$ denote the coset space. Define

$$\phi_H : G \longrightarrow Sym(G/H)$$

by the rule

$$g\phi_H : Hh \mapsto Hhg,$$

for all $h \in G$. Let $\phi : G \longrightarrow Sym(X)$ be a transitive permutation representation of G. Then ϕ is equivalent to ϕ_H for some subgroup H of G. This identification now gives us a more practical way of computing minimal faithful permutation representations of groups. One needs to find a collection of subgroups $H_1, \ldots, H_n$ of G such that the intersection of the cores of the $H_i's$ is trivial. The minimal degree is then simply given by

$$\mu(G) = \min\left\{ \sum_{i=1}^{n} |G : H_i| \;\middle|\; \bigcap_{i=1}^{n} \operatorname{core}(H_i) = \{1\}\right\}.$$

From now on, we shall think of permutation representations of G as a disjoint union of $Sym(G/H_i)$ where $i = 1, 2, \ldots, n$.

2. Exceptional groups

Now we define the key notion of an exceptional group. A group G is said to be *exceptional* if it has a normal subgroup N with quotient G/N such that $\mu(G) < \mu(G/N)$. In this case, N is a *distinguished subgroup* with G/N the *distinguished quotient*. At a first glance, one may think such a definition is silly since if H is a subgroup of G, then necessarily $\mu(H) \leq \mu(G)$. However, by analogy to the example in [6], the author found an instance where this fails in spectacular fashion. Let $G = Q_8 \times Q_8 \times \ldots \times Q_8 = Q_8{}^n$ be the product of n copies of the quaternion group and let

$$N = \langle (z, z, 1, \ldots, 1), (1, z, z, 1, \ldots, 1), \ldots, (1, \ldots, z, z) \rangle,$$

where $z \neq 1$ is central. We have $\mu(G) = n\mu(D_8) = 4n$. But then $\mu(G/N) = 2^{n+1}$. This example shows that not only is the minimal degree of the distinguished quotient potentially larger than the minimal degree of the group, but in some cases it increases exponentially with the size of the group. Here is a result due to Easdown and Praeger (1988) concerning the smallest exceptional groups:

Proposition 1. *There are no exceptional groups of order strictly less than 32. The two exceptional groups of order* 32 *are:*

$$G = \langle x, y \mid x^8 = y^4 = 1, \; x^y = x^{-1} \rangle$$

with minimal degree 12, *with distinguished quotient*

$$G/\langle x^4 y^2 \rangle \cong \langle x, y \mid x^8 = y^4 = 1, \; y^2 = x^4, \; x^y = x^{-1} \rangle$$

of minimal degree 16 *and*

$$H = \langle x, y, n \mid x^8 = y^4 = n^2 = 1, \ y^2 = x^4, \ x^y = x^{-1}n, \ n^x = n^y = n \rangle$$

with minimal degree 12, *also with distinguished quotient*

$$H/\langle n \rangle \cong \langle x, y \mid x^8 = y^4 = 1, \ y^2 = x^4, \ x^y = x^{-1} \rangle$$

of minimal degree 16.

Proof. See [4]. □

This example motivated the study of how small exceptional groups could actually be for a general prime p. This was what Lemiuex later worked on.

3. Theory of Johnson, Wright and Lemieux

For the remainder of this paper, p will denote an odd prime. The minimal degree problem for groups was first investigated by Johnson in [1]. He set the foundations for the this area of study and established some major theorems. A few years later, Wright, in [2], found a neat formula for the minimal degrees of direct products p-groups. In [5] Lemieux showed that there are no exceptional p-groups of order strictly less than p^5. Then in [3], he demonstrated the existence of an exceptional group of order p^5. This section addresses without proof, (references to the relevant sourse are given) the contributions of the three authors. The following theorems are due to Johnson.

Theorem 1. *Let G be a non-trivial p-group whose centre Z is minimally generated by d elements, and let $\mathscr{R} = \{G_1, \ldots, G_n\}$ be a minimal (faithful) repesentation of G. Then for p an odd prime, we have $n = d$.*

Proof. See [1] □

Theorem 2. *Let G be a non-abelian p-group which does not decompose as a non-trivial direct product and whose centre is either cyclic or elementary abelian. Then we have the following bound:*

$$p\mu(Z) \leq \mu(G) \leq \frac{1}{p}|G : Z|\mu(Z).$$

Proof. See [1] □

The next theorem is Wright's main result.

Theorem 3. *Let G and H be p-groups. Then $\mu(G \times H) = \mu(G) + \mu(H)$.*

Proof. Wright actually proved this for all nilpotent groups and for all primes p, see [2]. □

Lemieux in [5] studied small exceptional p-groups. Although he could not find the smallest exceptional p-groups, he severely limited the existence of such groups in the following theorem:

Theorem 4. *There are no exceptional p-groups of order strictly less than p^5. If there are any exceptional p-groups of order p^5, then they must be a central extension of these 4 isomorphism classes of distinguished quotients which are p-groups of order p^4 :*

$$G_1 = \langle x, y, z \mid x^{p^2} = y^p = z^p = 1,\ [x,y] = 1,\ [x,z] = 1,\ [y,z] = x^p \rangle$$

$$G_2 = \langle x, y, z \mid x^{p^2} = y^p = z^{p^2} = 1,\ z^p = x^p,\ [x,y] = x^p,\ [x,z] = y,\ [y,z] = 1 \rangle$$

$$G_3 = \langle x, y, z \mid x^{p^2} = y^p = z^{p^2} = 1,\ z^p = x^{\alpha p},\ [x,y] = x^p,\ [x,z] = y,\ [y,z] = 1 \rangle$$

$$G_4 = \langle x, y, z, w \mid x^p = y^p = z^p = w^p = 1,\ [x,y] = z,\ [x,z] = [x,w] = [y,z] =$$
$$[y,w] = [z,w] = 1 \rangle$$

where α is a quadratic non-residue mod p.

In [3] Lemiuex showed the existence of an exceptional group of order p^5 with distinguished quotient isomorphic to G_1. The remaining cases will be examined in the next section.

4. The remaining cases

Theorem 5. *Here are three exceptional p-groups of order p^5 and minimal degree $2p^2$:*

$$E_1 = \langle x, y, z, n \mid x^{p^2} = y^p = z^p = n^p = 1,\ [y,z] = x^p n^{-1},\ [x,z] = n,$$
$$[x,y] = [x,n] = [y,n] = [z,n] = 1 \rangle$$

$$E_2 = \langle x, y, z, n \mid x^{p^2} = y^p = z^{p^2} = n^p = 1,\ x^p = z^p n,\ [x,y] = x^p,$$
$$[x,z] = y,\ [y,z] = [x,n] = [y,n] = [z,n] = 1 \rangle$$

$$E_3 = \langle x, y, z, n \mid x^{p^2} = y^p = z^{p^2} = n^p = 1,\ z^p = x^{\alpha p} n,\ [x,z] = yn,$$
$$[x,y] = x^p,\ [y,z] = [x,n] = [y,n] = [z,n] = 1 \rangle$$

with distinguished quotients isomorphic to G_1, G_2 and G_3 respectively.

Proof. That E_1 is exceptional with distinguished quotient G_1 was shown in [3]. We now show that E_2 is exceptional with distinguished quotient isomorphic to G_2. It is clear that $E_2/\langle n \rangle \cong G_2$. The centre of E_2 is $\langle x^p, n \rangle$, and so by Theorem 1, any minimal faithful permutation representation of E_2 must have two orbits. Let

$$H_1 = \langle x, y \rangle \cong \langle x, y \mid x^{p^2} = y^p = 1,\ [x,y] = x^p \rangle \qquad \text{and}$$
$$H_2 = \langle y, z \rangle \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_p$$

be subgroups of E_2 of order p^3. Observe that $H_1 \triangleleft E_2$ and $H_2 \not\triangleleft E_2$, so that $\mathrm{core}H_1 = H_1$ and $\mathrm{core}H_2 \neq H_2$. Therefore $|\mathrm{core}H_2| = 1, p$ or p^2.

If $|\mathrm{core}H_2| = 1$, then $\mathrm{core}H_1 \cap \mathrm{core}H_2 = \{1\}$ and we are done. Now suppose $|\mathrm{core}H_2| = p^2$ so that $\mathrm{core}H_2 \cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$. Thus without loss of generality, $\mathrm{core}H_2 = \langle z \rangle$ or $\langle zy \rangle$ or $\langle z^p, y \rangle$. However none of these are normal subgroups of E_2 since $[x, z] = y$, $(z^{-1}y^{-1})^x = z^{p-1}n$ and $(y^{-1})^x = z^p y^{-1} n$ respectively. Hence $|\mathrm{core}H_2| = p$, so that without loss of generality, $\mathrm{core}H_2 \cong \langle y \rangle$ or $\langle z^p \rangle$ or $\langle z^p y \rangle$. However of the three, only $\langle z^p \rangle \lhd E_2$. Hence $\mathrm{core}H_2 = \langle z^p \rangle = \langle x^p n^{-1} \rangle$. Whence we have

$$\mathrm{core}H_1 \cap \mathrm{core}H_2 = H_1 \cap \langle x^p n^{-1} \rangle = \{1\}.$$

Now we get

$$2p^2 = p\mu(Z(E_2)) \le \mu(E_2) \le |E_2 : H_1| + |E_2 : H_2| = p^2 + p^2 = 2p^2 < p^3 = \mu(G_2)$$

and so $\mu(E_2) = 2p^2$. The first inequality is by Theorem 2 and the last equality is in the content of table 1 in [3].

Now we proceed to show that E_3 is exceptional with distinguished quotient G_3. Firstly, it is obvious that $E_3/\langle n \rangle \cong G_3$. Observe that the centre of E_3 is $\langle x^p, n \rangle$, and so by Theorem 1, any minimal faithful permutation representation of E_3 must have two orbits. Let

$$S_1 = \langle x, y \rangle \cong \langle x, y \mid x^{p^2} = y^p = 1, \ [x, y] = x^p \rangle \qquad \text{and}$$

$$S_2 = \langle y, z \rangle \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_p$$

be the two subgroups of E_3 corresponding to the two orbits. We need to show that $\mathrm{core}S_1 \cap \mathrm{core}S_2 = \{1\}$. Note that $S_1 \ntriangleleft E_3$. Now observe that $\langle x^p, y \rangle$ is a maximal subgroup of S_1, of order p^2 and normal in E_3. Thus $\mathrm{core}S_1 = \langle x^p, y \rangle$. It is easy to see that $S_2 \ntriangleleft E_3$. If $|\mathrm{core}S_2| = p^2$, then without loss of generality we may assume $\mathrm{core}S_2 \cong \langle z \rangle$ or $\langle y, z^p \rangle$. Now neither $\langle z \rangle$ nor $\langle y, z^p \rangle$ are normal in E_3. Thus $|\mathrm{core}S_2| = p$ and we conclude without loss of generality that $\mathrm{core}S_2 \cong \langle z^p \rangle$. Now

$$\mathrm{core}S_1 \cap \mathrm{core}S_2 = \langle x^p, y \rangle \cap \langle z^p \rangle = \langle z^p n, y \rangle \cap \langle z^p \rangle = \{1\}.$$

So we have

$$2p^2 = p\mu(Z(E_3)) \le \mu(E_3) \le |E_2 : S_1| + |E_2 : S_2| = p^2 + p^2 = 2p^2 < p^3 = \mu(G_3),$$

and so $\mu(E_3) = 2p^2$ and we are done. $\qquad\square$

Note that the group G_4 was omitted from the considerations of the theorem. Now we will prove that G_4 does not centrally extend to an exceptional group of order p^5.

Theorem 6. *Centrally extending the group G_4 will not result in an exceptional p-group E_4 of order p^5, with distinguished quotient isomorphic to G_4.*

Proof. Let E_4 be an extension of G_4 satisfying the conditions of the theorem. First we show that $Z(E_4) \cong \langle n \rangle$, where $E_4/\langle n \rangle \cong G_4$. If $p^2 \le |Z(E_4)|$, then by Theorem 2, we have $\mu(E_4) \ge 2p^2 > p^2 + p = \mu(G_4)$, contradicting that

E_4 is exceptional. Hence we must have $|Z(E_4)| = p$ and thus $Z(E_4) = \langle n \rangle$. Hence the permutation representation is transitive with $\mu(E_4) = |E_4 : K|$ for some subgroup $K \leq E_4$. Clearly we must have $\mu(E_4) > p$. We must show that $\mu(E_4) > p^2$. Suppose not, so that $\mu(E_4) = p^2$. Then $\mu(E_4) = |E_4 : K|$, where K is a core-free subgroup of order p^3 in E_4. We have from 4.4 in [8] that K is isomorphic to either one of the following 5 groups:

$$\mathbb{Z}_{p^3}, \ \mathbb{Z}_p^2 \times \mathbb{Z}_p, \ \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p, \ H = \langle x, y \mid x^{p^2} = y^p = 1, \ [x,y] = x^p \rangle \text{ or}$$
$$L = \langle x, y, z \mid x^p = y^p = z^p = 1, \ [x,y] = z, \ [x,z] = [y,z] = 1 \rangle.$$

Since $\mu(K) \leq \mu(E_4) = p^2$, it follows that K cannot be isomorphic to $\mathbb{Z}_{p^3}$ or $\mathbb{Z}_p^2 \times \mathbb{Z}_p$. If K is isomorphic to either H or L, then since K is a core-free subgroup of E_4, it follows that both H and L intersects trivially with $\langle n \rangle$ so that $H \times \langle n \rangle$ and $L \times \langle n \rangle$ are internal direct products. Now

$$\mu(H \times \langle n \rangle) = \mu(L \times \langle n \rangle) = p^2 + p \leq \mu(E_4) = p^2,$$

a contradiction. So we are left with the remaining case that $K \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$. By a result from [7], there exists an abelian normal subgroup B of order p^3 in E_4. But since K does not contain any non-trivial normal subgroups of E_4, we have $K \cap B = \{1\}$, so we may form the semidirect product $B \rtimes K$. Moreover, $B \rtimes K$ is a subgroup of E_4. But then $|B \rtimes K| \geq p^6 > p^5 = |E_4|$, a contradiction. The proof is now complete. □

References

[1] D.L. Johnson, *Minimal permutation representations of finite groups*, American Journal of Mathematics **93** (1971), 857-866.

[2] D. Wright, *Degrees of Minimal Embeddings for Some Direct Products*, American Journal of Mathematics **79** (1975), 897-903.

[3] S. Lemieux, *Finite Exceptional p-Groups of Small Order*, Communications in Algebra **35** (2007), 1890-1894.

[4] D. Easdown and C.E. Praeger, *On minimal faithful permutation representations of finite groups*, Bulletin of the Australian Mathematical Society **38** (1988), 207-220.

[5] S. Lemiuex, *On minimal faithful permutation representations of finite groups*, M.Sc. thesis, Carlton University (1999)

[6] P.M. Neumann, *Some algorithms for computing with finite permutation groups*, Proceedings of groups- St Andrews (1986)

[7] W. Burnside, *Theory of groups of finite order*, Dover Publications, Inc., New York (1955)

[8] M. Hall, *Theory of groups*, The Macmillan Company (1959)